Quantum Computation:
Zusammenfassung der 3. Vorlesung (06.05.2011)

1.2 *Quantenrechner, unitäre Gatter*

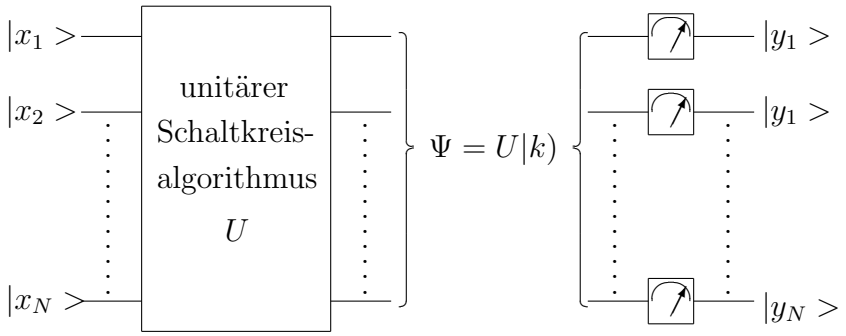
An die Stelle von Funktoren der Aussagenlogik treten bei Quantenrechnern unitäre Operatoren, weil die Manipulation der Qubitzustände durch äußere Wechselwirkungen der Schrödingerdynamik unterliegt. Die von 0 bis $N-1$ numerierten Elemente der Computerbasis schreiben wir un der Form

$$|k) = |x_1 2^{N-1} + x_2 2^{N-2} + \cdots + 2^0 x_N) = |x_1 x_2 \ldots x_N > .$$

Da die Schrödingerdynamik reversibel ist, muss im Gegensatz zu klassischen Rechnern die Anzahl N der eingegeben Qubits mit der Anzahl der resultierenden Qubits übereinstimmen. Eingegeben wird im Allgemeinen ein Zustand $|k)$, der dem k-ten klassischen Wort entspricht. Das Ergebnis eines Rechnerlaufs wird durch Messung der Observablen

$$A = \sum_1^{N-1} k|k)(k|$$

erhalten, das zufällig sein kann. Das Schema des Quantenrechners ist



1.2.1 *Elementare unitäre Gatter, Universalität*

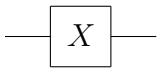
Wie bei klassischen Algorithmen, lassen sich auch die unitären Algorithmen mit elementaren, 1-Qubit- und 2-Qubitgattern erzeugen.

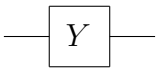
1.2.1.1 *1-Qubitgatter*

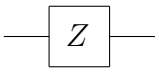
An die Stelle der vier klassischen monadischen Gatter tritt die vierdimensionale Gruppe der unitären $\mathbf{C}^2$ Transformationen, die $U(2)$. Jede unitäre 2×2-Matrix lässt sich in der Form [

$$U = e^{i\alpha} R, \quad \alpha \in \mathbf{R}, \qquad R \in U(2)$$

schreiben. Die dreidimensionale Untergruppe der Spindrehungen, die $SU(2)$, wird von den Paulimatrizen erzeugt. Die zugehörigen Gatter heißen Pauli-Gatter:



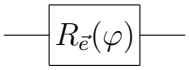




$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Sie sind hermitesch und unitär, haben aber die Determinante -1. Mit i muiltipliziert gehören sie der $SU(2)$ an und stellen die Spindrehungen, d.h. die räumlichen Drehungen des Dralls, den wir durch den Blochvektor veranschaulicht haben, mit dem Winkel π in positiver Richtung um die jeweilige Koordinatenachse dar. Mit den Polarkoordinaten Θ und Φ der Drehachse $\mathbf{e}(\Theta, \Phi)$ und dem Drehwinkel φ ist das Gittersymbol dür die allgemeine Spindrehung

allg. Spindrehung



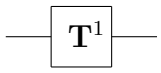
$$R_{\vec{e}}(\varphi) = e^{-i\frac{\varphi}{2}(\vec{e}\cdot\vec{\sigma})}$$

Die aufsummierte Exponentialreihe ist

$$R_{\vec{e}}(\varphi) = e^{-i\frac{\varphi}{2}(\vec{e}\cdot\vec{\sigma})} = \cos(\frac{\varphi}{2})\mathbf{1} - i\sin(\frac{\varphi}{2})(\vec{e}\cdot\vec{\sigma}).$$

Die Gatter der eindimensionalen Untergruppe der Phasenfahtoren, die Torusgruppe, heißen Torusgatter

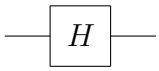
Torusgatter



$$e^{i\alpha}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

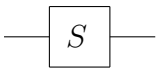
und entsprechen der Identität im klassischen Fall. Weitere ausgezeichnete Gatter sind:

Hadamard Gatter



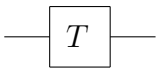
$$H = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Phasengatter



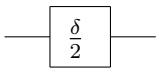
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$\frac{\pi}{8} - Gatter$



$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

$\frac{\delta}{2} - Gatter$



$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}$$

Weshalb das Phasengatter auch $\frac{\pi}{4}$-Gatter und T auch $\frac{\pi}{8}$-Gatter genannt wird, hat möglicherweise historische Gründe: Man kann diese Matrizen auch als $SU(2)$ Matrizen mit dem entsprechenden Phasenfaktor schreiben. Wir werden diese Konvention bei der Definition des $\frac{\delta}{2}$-Gatters beibehalten.

Wir bertrachtn nun die Wirkung der allgemeinen Spindrehungen,

$$R_{\vec{e}}(\varphi) = \cos(\frac{\varphi}{2})\mathbf{1} - i\sin(\frac{\varphi}{2})(\vec{e}\cdot\vec{\sigma}),$$

auf die Qubitzustände etwas genauer. Mit Hilfe der Formel

$$(\vec{x}\cdot\vec{\sigma})(\vec{y}\cdot\vec{\sigma}) = (\vec{x}\cdot\vec{y})\mathbf{1} + i(\vec{x}\times\vec{y})\cdot\vec{\sigma},$$

aus der zunächst

$$[(\vec{r}\cdot\vec{\sigma}),(\vec{e}\cdot\vec{\sigma})] = i(\vec{r}\times\vec{e}-\vec{e}\times\vec{r})\cdot\vec{\sigma} = 2i(\vec{r}\times\vec{e})\cdot\vec{\sigma}$$

und dann

$$\begin{aligned}(\vec{e}\cdot\vec{\sigma})(\vec{r}\cdot\vec{\sigma})(\vec{e}\cdot\vec{\sigma}) &= (\vec{e}\cdot\vec{\sigma})((\vec{e}\cdot\vec{\sigma})\,(\vec{r}\cdot\vec{\sigma}) + 2i(\vec{r}\times\vec{e})\cdot\vec{\sigma}) \\ &= \vec{r}\cdot\vec{\sigma} - 2(\vec{e}\times(\vec{r}\times\vec{e}))\cdot\vec{\sigma} \\ &= \vec{r}\cdot\vec{\sigma} - 2(\vec{r}-(\vec{e}\cdot\vec{r})\vec{e}))\cdot\vec{\sigma} \\ &= (2(\vec{e}\cdot\vec{r})\vec{e}-\vec{r})\cdot\vec{\sigma},\end{aligned}$$

berechnet man

$$\begin{aligned}R_{\vec{e}}(\varphi)(\vec{r}\cdot\vec{\sigma})R^{+}_{\vec{e}}(\varphi) &= \cos^2(\frac{\varphi}{2})(\vec{r}\cdot\vec{\sigma}) + i\cos(\frac{\varphi}{2})\sin(\frac{\varphi}{2})[(\vec{r}\cdot\vec{\sigma}),(\vec{e}\cdot\vec{\sigma})] \\ &\quad + \sin^2(\frac{\varphi}{2})(\vec{e}\cdot\vec{\sigma})(\vec{r}\cdot\vec{\sigma})(\vec{e}\cdot\vec{\sigma}) \\ &= \cos^2(\frac{\varphi}{2})(\vec{r}\cdot\vec{\sigma}) - 2\cos(\frac{\varphi}{2})\sin(\frac{\varphi}{2})(\vec{r}\times\vec{e})\cdot\vec{\sigma} \\ &\quad + \sin^2(\frac{\varphi}{2})(2(\vec{e}\cdot\vec{r})\vec{e}-\vec{r})\cdot\vec{\sigma} \\ &= \cos(\varphi)(\vec{r}\cdot\vec{\sigma}) + (1-\cos\varphi)(\vec{e}\cdot\vec{r})(\vec{e}\cdot\vec{\sigma}) \\ &\quad - \sin(\varphi)(\vec{r}\times\vec{e})\cdot\vec{\sigma}.\end{aligned}$$

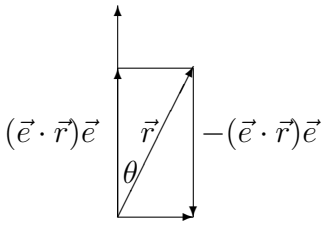
Damit folgt

$$R_{\vec{e}}(\varphi)\frac{1}{2}(\mathbf{1}+\vec{r}\cdot\vec{\sigma})R^{+}_{\vec{e}}(\varphi) = \frac{1}{2}(\mathbf{1}+\vec{s}\cdot\vec{\sigma}),$$

wobei

$$\vec{s} = \cos(\varphi)(\vec{r}-(\vec{e}\cdot\vec{r})\vec{e}) + \sin(\varphi)(\vec{e}\times\vec{r}) + (\vec{e}\cdot\vec{r})\vec{e}$$

ist. Bedenkt man, dass die drei Vektoren $\vec{e}$, $(\vec{r}-(\vec{e}\cdot\vec{r})\vec{e})$, und $(\vec{e}\times\vec{r})$ paarweise orthogonal sind und in dieser Reihenfolge ein rechtsorientiertes System bilden, und ferner, dass $\|\vec{r}-(\vec{e}\cdot\vec{r})\vec{e}\| = \|\vec{e}\times\vec{r}\| = r\sin(\theta)$ gilt, wobei θ der von $\vec{e}$ und $\vec{r}$ eingeschlossene Winkel ist, dann sieht man leicht, dass der Blochvektor eine Drehung in positiver Richtung um die $\vec{e}$-Achse mit dem Winkel φ erfährt:



$(\vec{e},\vec{r})$-Ebene

Die skizzierte Figur wrd um den Winkel φ in der $((\vec{r}-(\vec{e}\cdot\vec{r})\vec{e}),(\vec{e}\times\vec{r}))$-Ebene gedreht. Sei $D_{\vec{e}}(\varphi)\in SO(3)$ die Drehmatrix, die Drehuungen um $\vec{e}$ in positiver Richtung erzeugt, dann gilt also

$$\vec{s}=D_{\vec{e}}(\varphi)\vec{r}\quad\text{bzw.}\quad R_{\vec{e}}(\varphi)\frac{1}{2}(\mathbf{1}+\vec{r}\cdot\vec{\sigma})R^{+}_{\vec{e}}(\varphi)=\frac{1}{2}(\mathbf{1}+(D_{\vec{e}}(\varphi)\vec{r})\cdot\vec{\sigma}).$$

Topologisch ist die $SU(2)$ die zweifache und universelle Überlagerungsgruppe der $SO(3)$. Dies äußert sich auch darin, dass $R_{\vec{e}}(2\pi)=-\mathbf{1}$ und erst $R_{\vec{e}}(4\pi)=\mathbf{1}$ ist. Beim Blochvektor fällt der Phasenfaktor heraus und er transformiert sich nach der $SO(3)$. Dies macht nicht nur für reine Qubit-ZUstände, $\|\vec{r}\|=1$, sonder auch für statistische Gemische, $\|\vec{r}\|<1$, Sinn, denn die Komponenten einer reinen Zerlegung unterliegen der Spindrehung, wobei die Mischunngsverjältnisse unverändert bleiben.

In der Kreiseltheorie wird die Konfiguration eines starren Körpers mit einem raumfesten Körperpunkt durch die ´drei Eulerschen Winkel (Φ,Θ,Ψ) ausgedrückt. Dazu benötigt man nur Drehmatrizen, die Drehungen un die Koordinatenachsen eines cartesischen Koordinatensystems erzeugen. Der Einfachheit halber seien diese mit $D_x(\varphi)$, $D_y(\varphi)$ und $D_z(\varphi)$ bezeichnet. Die Drehmatrix, die die Körperpunkte von einer Ursprungslage in die betrachtete Konfiguration abbildet, ist dabei

$$K(\Phi,\Theta,\Psi)=D_z(\Psi)D_x(\Theta)D_z(\Phi).$$

Dazu stellt man sich ein körperfestes Dreibein vor, das mit dem raunfesten in der Ursprungslage zusammenfällt. Der Körper wird zunächst mit dem Winkel Φ um seine z-Achse, dann um seine im Raum gedrehte x-Achse und schließlich um seine im Raum veränderte z-Achse in positiver Richtung gedreht. Wendet man dies auf die Punkte der Blochkugel als starren Körper an, dann transformiert sich ein Blochvektor $\vec{r}$ mit den entsprechenden

Spindrehungen $R_z(\Phi)$, $R_x(\Theta)$ und $R_z(\Psi)$ nach

$$\vec{s}\cdot\vec{\sigma} = (K(\Phi,\Theta,\Psi)\vec{r})\cdot\vec{\sigma} = R_z(\Psi)R_x(\Theta)R_z(\Phi)(\vec{r}\cdot\vec{\sigma})R_z^+(\Phi)R_x^+(\Theta)R_z^+(\Psi).$$

Auf dieser Grundlage beweist man den Satz, mit dessen Hilfe wir weiter unten zeigen werden, dass die 1-Qubitgatter zusammen mit einem bestimmten 2-Qubitgatter bereits eine universelle Menge elementarer Gatter bilden.

Satz: Sei $U \in U(2)$, dann gibt es Spindrehungen A, B und C und einen Phasenfaktor $e^{i\alpha}$, so dass

$$ABC = \mathbf{1} \qquad \text{und} \qquad e^{i\alpha}A\sigma_x B\sigma_x C = U$$

gelten.

Beweis: Die Gleichung $ABC = \mathbf{1}$ wird offensichtlich von

$$A := R_z(\Psi)R_y(\frac{\Theta}{2}), \quad B := R_y(-\frac{\Theta}{2})R_z(-\frac{\Psi+\Phi}{2}), \quad C := R_z(-\frac{\Psi-\Phi}{2})$$

erfüllt. Ferner gilt

$$\sigma_x B\sigma_x = \sigma_x R_y(-\frac{\Theta}{2})\sigma_x\sigma_x R_z(-\frac{\Psi+\Phi}{2})\sigma_x = R_y(\frac{\Theta}{2})R_z(\frac{\Psi+\Phi}{2}),$$

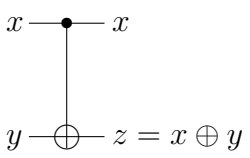
denn σ_x stellt eine Spindrehung mit dem Winkel π um die x-Achse der Blochkugel dar, die $\vec{e}_y \mapsto -\vec{e}_y$ und $\vec{e}_z \mapsto -\vec{e}_z$ zur Folge hat. Rechnerisch kann man das auch mit

$$\sigma_x R_y(-\frac{\Theta}{2})\sigma_x = \sigma_x e^{i\frac{\Theta}{4}\sigma_y}\sigma_x = e^{i\sigma_x\frac{\Theta}{4}\sigma_x\sigma_y\sigma_x} = e^{-i\sigma_x\frac{\Theta}{4}\sigma_y} = R_y(\frac{\Theta}{2})$$

und ensprechend für R_z bestätigen. Die behauptete Gleichung $e^{i\alpha}A\sigma_x B\sigma_x C = U$ folgt dann unmittelbar.

1.2.1.2 *2-Qubitgatter*

Bei gesteuerten Gattern werden ein oder mehrere Bits, die dabei unverändert bleiben, dazu benutzt, um einen Algorithmus zu steuern. Der einfachste Fall ist die gesteuerte Negation:

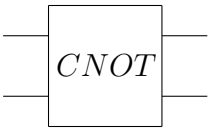


	xy	xz	
0	00	00	0
1	01	01	1
2	10	11	3
3	11	10	2

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 2 \end{pmatrix} = (23)$$

CNOT *Wahrheitswerttabelle* *ewrzeugte Permutation*

Dieses Gatter ist offenbar reversibel und erzeugt die Transposition (23) in der Permutationsgruppe S_4. Auf die Basiselemente der Computerbasis angewendet, entsteht das unitäre $CNOT$-Gatter:

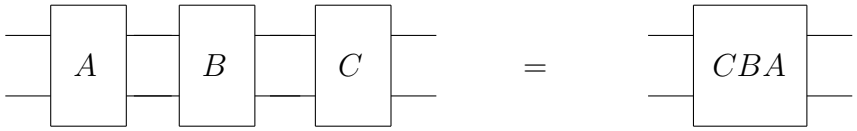


$$(\,|0)\,|1)\,|2)\,|3)\,)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} (0| \\ (1| \\ (2| \\ (3| \end{pmatrix}$$

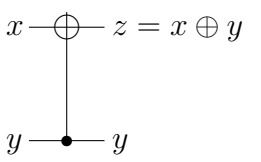
Es erzeugt im $\mathbf{C}^2$ die Transformation

$$\Psi = (\,|0)\,|1)\,|2)\,|3)\,)\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \mapsto (\,|0)\,|1)\,|2)\,|3)\,)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix},$$

so dass für das Zusammensetzen von Gattern in Schaltkreisen die Rechenregel



gilt. Eine weitere gesteuerte Negation ist:



	xy	zy	
0	00	00	0
1	01	11	3
2	10	10	2
3	11	01	1

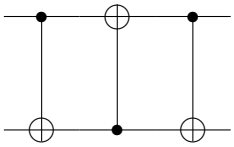
$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 2 & 1 \end{pmatrix} = (13)$$

CNOT' *Wahrheitswerttabelle* *erzeugte Permutation*

in der Computerbasis wird sie durch die Permutationsmatrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

dargestellt. Man rechnet leicht nach, dass die Matrix zur folgenden Kombination von $CNOT$-Gattern

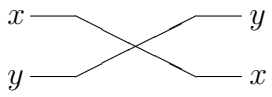


$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

SWAP

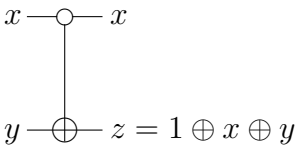
ist. Dabei kann man eine Regel für die Multiplikation mit Permutationsmatrizen ausnutzen: Sei P eine Permutationsmatrix, d.h. in jeder Zeile sowie in jeder Spalte stehen außer Nullen genau eine Eins, und A eine andere Matrix. Bei Linksmultiplikation mit P werden lediglich die Zeilen von A permutiert, bei Rechtsmultiplikation lediglich die Spalten. Die betrachtete Gatterkombination erzeugt die Transposition (12). An der Wahrheitswerttabelle sieht man, dass dies einer Vertauschung der Qubits gleichkommt, wodurch der Name gerechtfertigt wird:

	xy	yx	
0	00	00	0
1	01	10	2
2	10	01	1
3	11	11	3



SWAP

Eine weitere Version der gesteuerten Verneinung entsteht dadurch, dass die Verneinung durch 0 ausgelöst wird:



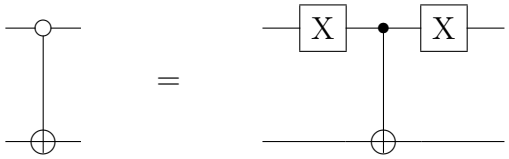
	xy	xz	
0	00	01	1
1	01	00	0
2	10	10	2
3	11	11	3

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

CNOT" *Wahrheitswerttabelle* *Permutationsmatrix*

Die vorstehenden Versionen der gesteuerten Verneinung mit ihrer Kombination zum $SWAP$-Gatter enthalten die drei Transpositionen benachbarter Elemente von (0 1 2 3). Damit können alle Permutationen der S_4 bzw. die 24 (4×4)-Permutationsmatrizen erzeugt werden.

Nun gilt offenbar:



Ferner folgt mit

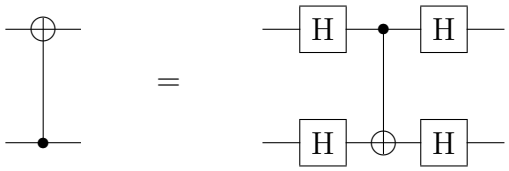
$$H \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} H & H \\ H & -H \end{pmatrix},$$

dass

$$\frac{1}{2}\begin{pmatrix} H & H \\ H & -H \end{pmatrix}\begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & X \end{pmatrix}\begin{pmatrix} H & H \\ H & -H \end{pmatrix} =$$

$$\frac{1}{2}\begin{pmatrix} H & H \\ H & -H \end{pmatrix}\begin{pmatrix} H & H \\ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} & \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ o & 1 & 0 & 0 \end{pmatrix}$$

gilt. Also gilt ferner:



Bis hierher zusammenfassend, können wir den folgenden Satz behaupten.

Satz: Mit den 1-Qubitgattern X, H und dem 2-Qubitgatter $CNOT$ können alle (4×4) Permutationsmatrizen erzeugt werden.

Die Aussage des Satzes ist von großer Bedeutung für die Implementation beliebiger unitärer Matrizen mitelementaren Gattern. Sie zeigt auch, dass reversiblen klassischen Gattern unitäre Quantengatter entsprechen.